SOFTWARE CONNECTORS TO CLOUDFLARE'S NETWORK

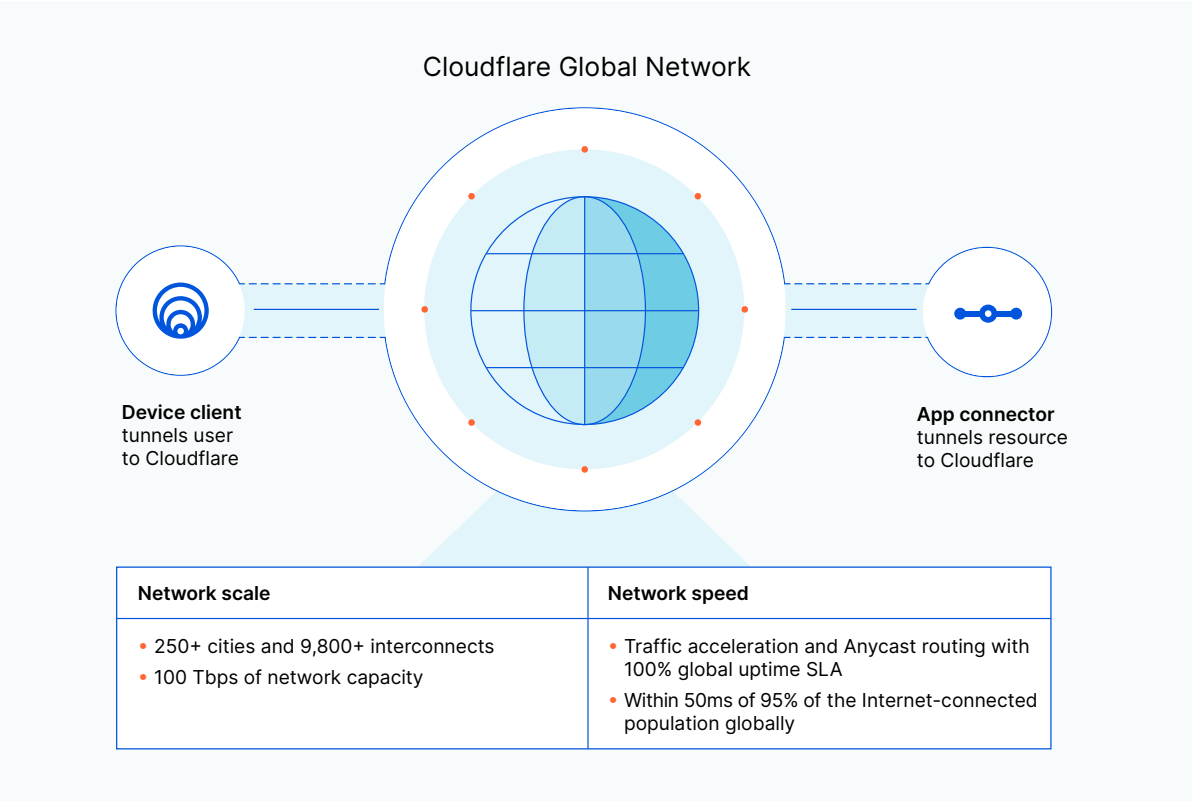
CLOUDFLARE

Onboard users and resources to our Zero Trust platform with ease and flexibility

Determining how best to send traffic to a provider's network is critical to progressing with Zero Trust.

While organizations can use their existing on-premise equipment (like GRE tunnels) to direct traffic to Cloudflare's network, many customers deploy our lightweight software to establish those connections — **specifically, our application connector and device client**. Both are linchpins of our Zero Trust platform (Cloudflare for Teams) that organizations use to create encrypted tunnels to our network, thereby securing their users and resources.

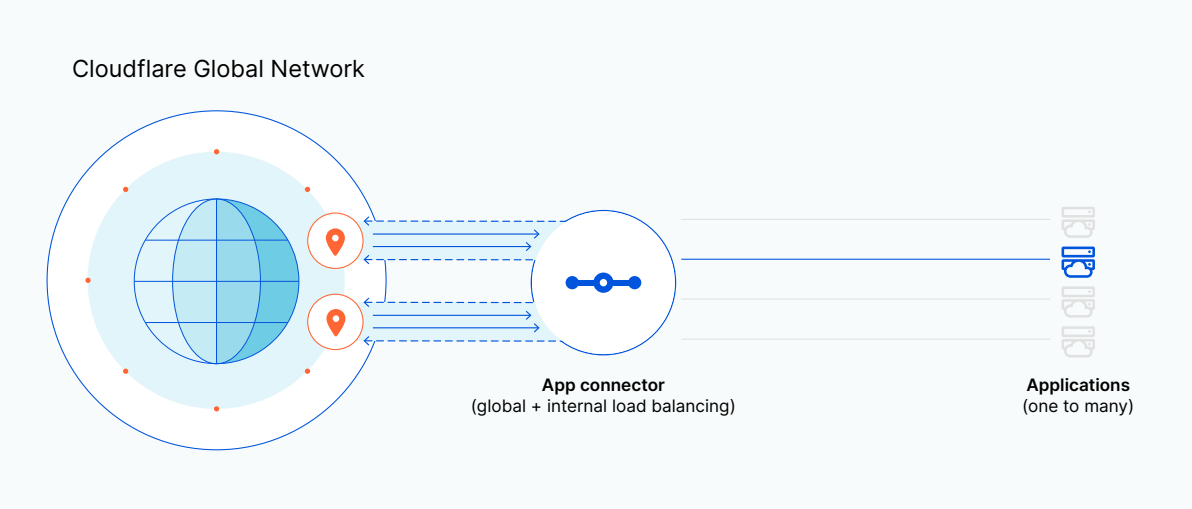
Cloudflare for Teams is priced per user, not the number of app connectors or tunnels deployed. In fact, we offer unlimited tunnel connections and bandwidth, so you can focus on delivering security in the way your organization needs it.



Network scale	Network speed
• 250+ cities and 9,800+ interconnects • 100 Tbps of network capacity	• Traffic acceleration and Anycast routing with 100% global uptime SLA • Within 50ms of 95% of the Internet-connected population globally

Secure connections that tunnel from your apps to our network

Creating, routing, and running tunnel connections to our network is straightforward with our app connector, which runs as a lightweight daemon in your infrastructure. Connectors are flexible, allowing you to connect to one or many applications, and all traffic to those apps is routed through Cloudflare, where we apply identity-aware, default-deny controls.



Connecting to the Cloudflare network

- Each connector makes simultaneous outbound-only connections to 4 different servers in the closest 2 Cloudflare data centers to ensure reliability
- The connector is integrated with Cloudflare's global load balancer, which some of the largest Internet sites rely on to distribute traffic

Connecting to your apps

- One app connector can support one to many apps
- The same connector can maintain multiple instances simultaneously, enabling faster configuration changes without restarts or downtime

SOFTWARE CONNECTORS TO CLOUDFLARE'S NETWORK

Flexible deployment

- Run command-line tool as a service on Linux, Windows and macOS
- Pre-packaged as a Docker container
- Replica support for modern Kubernetes environments
- Use Terraform for automated deployment of tunnel connections

DDoS protection and traffic filters

- By default, access is protected by Cloudflare's cloud-native suite of global reverse proxy and private routing services, including authoritative DNS, load balancing, L4 FWaaS, and L7 DDoS mitigation (L4 DDoS is an add on)
- Using a single connector instance, ingress rules can locally proxy and filter traffic to multiple resources running on one server

Inline security inspection

- Add on more natively-integrated security services, including WAF, antivirus scanning, file type controls, and remote browser isolation.

Secure connections from users to our edge with our device client

Whether protecting remote or office employees, deploying device clients allows organizations to bring security controls to wherever users are. Cloudflare's client, WARP, is optimized for ease-of-use: both streamlined for admins to manage and unintrusive for end users to rely on.

Design strengths

Safer, faster protocol

- Our client uses a custom implementation of WireGuard, a modern protocol that establishes tunnels with more advanced encryption and higher speeds than IPsec or SSL, which are the default with traditional VPN clients.
- The relatively short code base is open source and auditable by your security team.

Always encrypted

- All traffic is encrypted from devices to our network — always. Ask around, and you'll learn that many clients using TLS or DTLS tunnels come with null encryption.

Enhanced compatibility

- Our client runs in the userspace of an operating system, not kernel space, therefore avoiding compatibility headaches with existing VPN clients and improving usability on unsupervised mobile devices.
- WARP works across all major operating systems (e.g. Windows, macOS, Linux, iOS, chromeOS, and Android). Our code base (in Rust) only ever requires minor tweaks across operating systems, and the vast majority is reused.

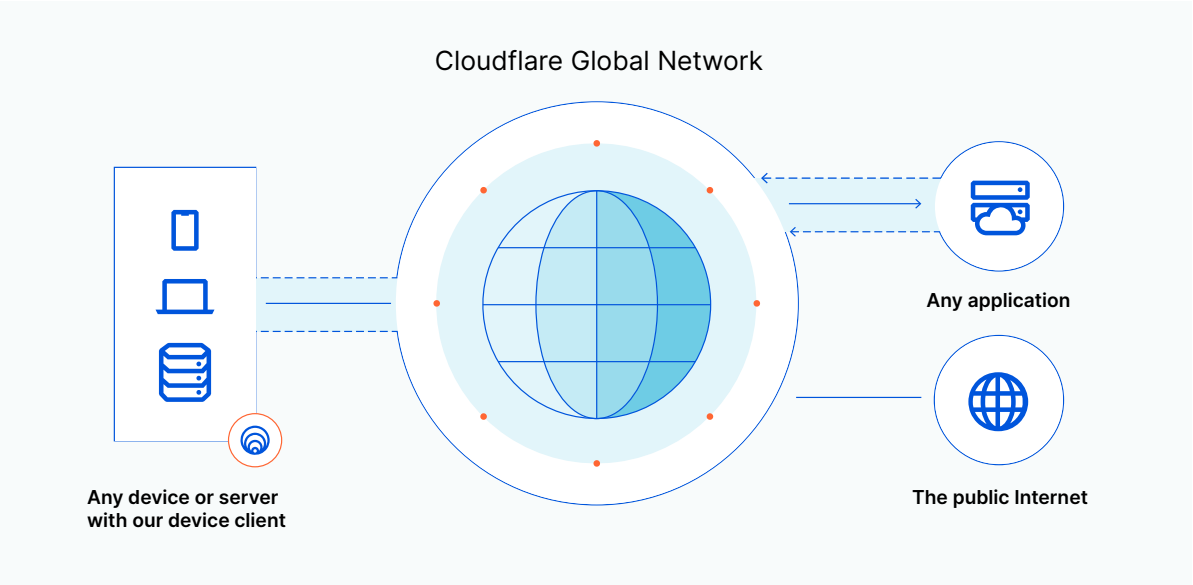
Tested and trusted by millions

- Our enterprise client shares the same code base as our consumer client, which is used daily by tens of millions worldwide. Testing for so many individual users means it comes more battle-ready than most clients used for Zero Trust.

Future-proof

- WARP fully supports IPv6-only home networks and 5G tethering to support our expanding, evolving Internet.

SOFTWARE CONNECTORS TO CLOUDFLARE'S NETWORK



Supporting flexibility in deployments

Our client is flexible across deployment approaches, so connections to our edge can fit your organization's needs and preferences:

Step 1: Enroll client

Managed or self-enrollment

- For managed devices, we offer streamlined workflows to deploy via popular mobile device management (MDM) softwares.
- If self-enrollment is ever needed, the entire process takes only a few minutes.

Step 2: Configure the client

Different modes for different needs

- The default mode sends traffic through WireGuard tunnels to enable identity-based policies, antivirus scanning, device posture, and other security features.
- Alternatively, use DNS over HTTPS for traffic you don't want sent through the default mode to apply DNS filtering and protect against WiFi eavesdroppers or rogue ISPs.
- Or use local proxy mode to encrypt traffic only from specific applications.

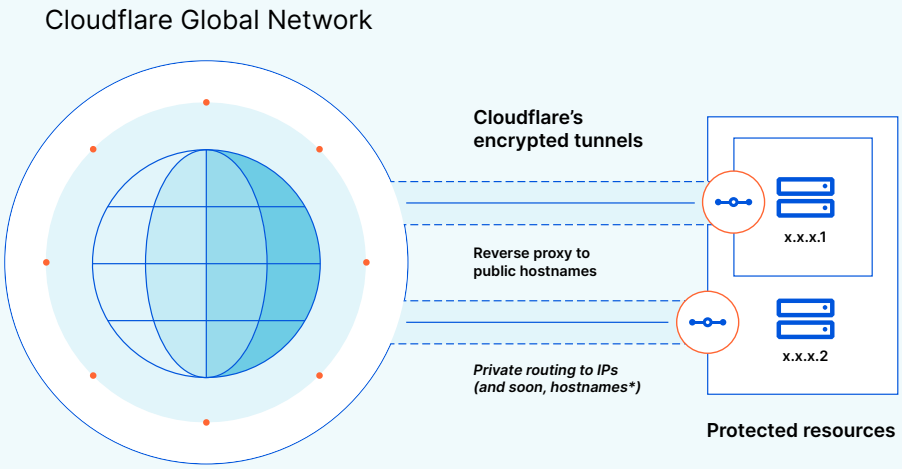
Split tunneling

- For any traffic you really do not want or need to send to our network, our client increasingly supports a wider range of split tunnelling features (by domain names and IP ranges today, and more coming soon). We give you final control.

Flexible deployment methods of our app connector and device client in action

Cloudflare sits in front of your applications to provide Zero Trust security. Deploying our app connector in front of your private applications creates an encrypted, outbound-only connection from your resources to our edge, where Cloudflare inspects traffic.

Our app connector locks down a wide range of apps in any environment. Tunnels are isolated from the Internet, and Cloudflare enforces default-deny policies based on identity and device posture.



Method 1: Connect to public hostname via a browser (clientless)

The first method does not require a device client and works best for web-, SSH- or VNC-based self-hosted apps

Our connector establishes tunnels between our edge and apps identified by their public hostnames.

All access requests to these named resources go through Cloudflare first to allow or deny traffic. This reverse-proxy motion leverages our long-standing strengths in DNS, WAF, and DDoS mitigation.

Method 2: Private routing to internal IPs via our device client

The second method, which requires a client, supports an unlimited number of on-prem legacy apps over any TCP (and soon, UDP) connection.

Here, the connector is configured to represent private IP addresses (and soon, hostnames), before tunneling to our edge.

Apps behind these internal IP spaces are protected with our integrated firewall services that enforce least privilege and identity-aware access.

**In the interim, Cloudflare enables a workaround using a DNS override policy.*

Send as much traffic as you want to Cloudflare without sacrificing security

Our position

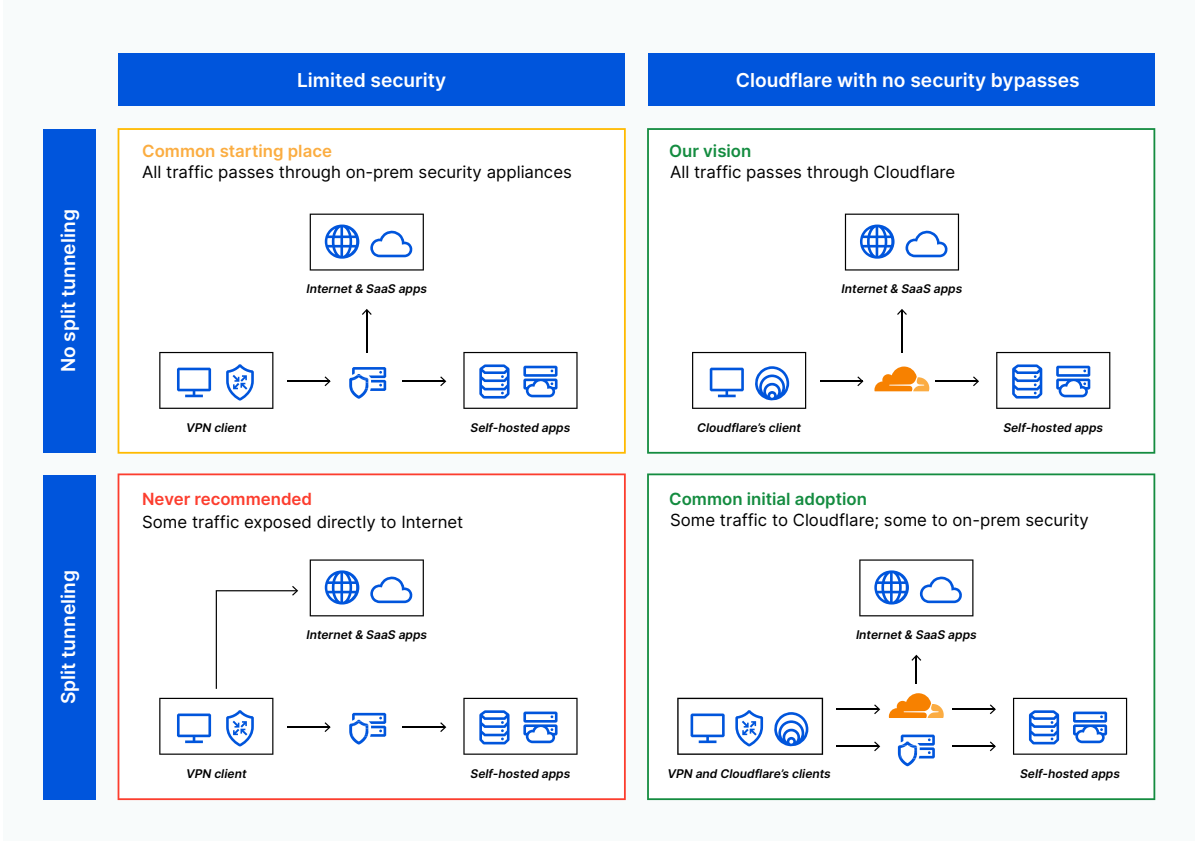
We believe that sending all traffic to Cloudflare over time maximizes visibility, protection, and performance for organizations.

Organizations initially adopting Cloudflare often take incremental steps by sending only some traffic to us at first and the rest through an existing security stack, whether on-prem or in the cloud. We are happy to help customers configure this type of 'split tunneling' so all traffic remains secured and consult with them on longer-term migration strategies.

A warning

However, we do warn organizations against a specific risky form of split tunneling: **namely, leaving one destination entirely unsecured**.

For example, organizations too often allow direct exposure to the public Internet to alleviate overburdened VPNs. That type of high-stakes, low visibility gamble — whether for convenience or a short-term performance boost — leaves a significant gap in an organization's journey to Zero Trust.



To learn more about our Zero Trust platform, Cloudflare for Teams, and request a demo or POC from a sales representative, please visit: https://www.cloudflare.com/teams/